The Netgear R7800 (X4S) Install Guide

- The Netgear R7800 (X4S) is a powerfull Atheros/Qualcomm based router with an IPQ8065 processor (https://www.qualcomm.com/products/ipq8065).
- Dual core Arm A9 based Qualcomm Krait 300 running both cores at 1,7 GHz, accompanied with a dual-core 800 MHz Network Subsystem (NSS) to accelerate packet processing
- Dual radio 2,4 GHz and 5 GHz , 4 stream MU-MIMO. Wave2
- 128 MB flash and 512 MB RAM
- Two USB 3.0 ports and one e-SATA port

See: https://wikidevi.com/wiki/Netgear_R7800

It is capable of near Gigabit speed LAN<>WAN throughput and about 100 Mb/s openVPN throughput depending on load and settings

Unpacking

Open the package to install the router, make a picture of the bottom for serial number, login credentials and MAC address.
Pull of the protective caps from the four antenna sockets.
Screw all 4 antennas on the router, antennas and sockets are marked, 2 antenna's with mark 1 at the back and antenna 2 an 3 in their respective sockets
Attach a wired client to the router, internet access is not necessary. Follow initial installation instructions, choose to manually setup your internet, set username and password.
Do **not** update the Netgear firmware, newer firmwares have a habit of restricting access or block third party software installation.
This install is done while using Netgear Genie firmware version1.0.2.46 which was installed on the router.
On the back of the router is a little switch, if flipped, it disables all LED lights except the power light.

Backup stock firmware

Backing up stock firmware and board data is a precautionary measure, and under normal circumstances and with mature DDWRT software it should not be necessary, So if you plan to keep using DDWRT and do not tinker with other firmwares (Voxel, OpenWRT, etc.) then you might consider skipping this step.
Backup by using built in backup is only somewhat useful as it actually only backups your settings, but can be done anyhow, (Netgear GUI: *ADVANCED/Administration/Backup Settings*).
Further backup methods can only be done through the Command Line Interface (CLI).
So you need a program like telnet which is standard on most Windows clients or download a more versatile program like putty (recommended).

1. If you intend to go back to stock and have the router in a difficult to access place, write down the serial number on the bottom of the router, you might need it.
2. Download and install: https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html
3. Unfortunately the CLI is not enabled by default on Netgear routers so the next step is to Enable the CLI:
    a. Easy method is to go to the debug page: https://192.168.1.1/debug.htm (change ip address according to IP address of router)
    There is a check box with "*enable telnet*", just tick it and you are good to go. This has to be repeated after every reboot.

b. If the enable telnet option is no longer available (sometimes newer firmware removes this option), you have to use a little utility called *telnetenable.exe* There are several, for some reading see:
https://wiki.openwrt.org/toh/netgear/telnet.console
https://github.com/insanid/NetgearTelnetEnable

I use tne, see: http://www.antinode.info/nte/index.html
Documentation is there, basically open a Dos command prompt, change directory to where the nte.exe is located and execute with:

nte m=50:6b:03:e9:ad:86 n=192.168.1.1 u=admin p=password

m= MAC address of the router which is on the box or on the underside of the router or when you go the the GUI of the router in Advanced/Router information.
n= IP address of the router
u= username you entered when configuring the router
p= password you entered when setting up the router.
(After reboot you have to do this again, you can make a batch file so that you do not have to type it in every time)

When you executed nte with the right parameters, you should see :
nte: Received ACK message.
Telnet access should be enabled, So telnet to your router and login with the username (contrary to DDWRT where the username is always *root*, you have to use the real username) and password, and you should see the prompt: #

4. Back up NVRAM parameters by copy/paste:
   a. *nvram show*
   b. Netgear stock has built in commands. The commands can be found in /sbin:
      cd /sbin
      ls
      Those commands can be usefull especially on Broadcom routers but are not needed on this router
   c. Sometimes useful can be to copy and paste the output of *dmesg*
   d. If you are planning to tinker with different firmwares then it is useful to backup your partitions, start with the following command to view all your partitions: *cat /proc/mtd* and copy and paste the output
   e. To copy the partitions, you need to *enable USB* on the Netgear Stock firmware. Netgear does not have the dd command which is available in DDWRT, instead you can use: *cat /dev/mtd6 > /tmp/mnt/sda2/mtd6_rootfs.bin* , which copies the seventh partition with rootfs. (you can view the mounted volumes with *mount,* I have 3 volumes on my USB stick)
      When you want to backup a partition from DDWRT, you can use the built in command for copying partitions: *dd if=/dev/mtd0 of=/opt/mtd0_boot.bin* , this copies the first boot partition to a file called mtd0_boot.bin in the /opt directory (which must be on a USB stick).

Installing DDWRT first Flash

There are firmware builds available from two different developers: Kong and Brainslayer (BS). Builds from both developers do however share the same code base (repository): https://svn.dd-wrt.com// , and both developers contribute to the code base although Brainslayer (BS) does the general maintenance and update of the code base.

So the differences are minor. Most important is that Kong only supports a fraction of available routers, and that gives him the ability to test his builds on his supported routers, Kong also has a regular and a test build, and he has an update utility for easy update with telnet.

Unfortunately since July 2019 Kong stopped development.
https://www.desipro.de/dd-wrt/Notice.txt, but his last build 40270 is, as for now, still a stable alternative:

Kong's builds for Atheros and Broadcom :
ftp://gakinaction.ddns.net/Kong%20PTB/3-23-2019/K3-AC-IPQ806X/
The latest Kong build is also included in this thread.

BS's builds can be found at: ftp://ftp.dd-wrt.com/ or if FTP is not available at https://dd-wrt.com/support/other-downloads/ look under BETAS).

My favourite builds: Kong 40270, BS 41075. BS 41174, BS 1328, BS 41517

First Flash

1. Some browser have problems with DDWRT GUI, I use good old Internet Explorer, clear browser cache as a first step.
2. Get Stock Netgear file your router (in case you have to go back): (https://www.netgear.com/support/product/R7800.aspx)
3. Get DDWRT file. For a first flash coming from stock you need a file ending with *.img*. Subsequent flashing can be done with files ending on *.bin*.
   For BS files go to *ftp://ftp.dd-wrt.com/betas/2019/* choose the build number of your liking and go the R7800 directory and load the *.img* files, not all users report success with files from BS, it probably depends on the used builds.
4. Use a wired client attached to your router, set this client to 192.168.1.10 net mask 255.255.255.0.
   Depending on your setup you have to leave your client at DHCP (see step 5)
5. Login to your router at 192.168.1.1. If you can not login go back to step 4 and leave your client to Automatically obtain IP address (DHCP).
6. *reset to defaults* via the Netgear stock GUI (*ADVANCED/Administration/Backup Settings/Revert to factory default settings*), click *Erase*, the router will reboot.
7. Login to the Netgear GUI at 192.168.1.1 and step through the first setup (it can take a while), choose manual configuration.
8. Upload DDWRT *.img* file via the GUI (*ADVANCED/Administration/Router update*), browse to where you downloaded the DDWRT file and click *Upload*.
   The router will reboot
9. After the reboot, point your browser to 192.168.1.1. and you should be greeted by a DDWRT login page asking to change username and password, set according to your wishes and click *Change Password*
10. Reboot router (it appears that you will not get access to the CLI without reboot)

11. Do a thorough cleaning of all remnants of the stock by using the CLI (telnet, putty) (remember username for CLI is always *root*) and do :
    nvram erase
    reboot
12. The router will reboot, login in with your web browser at 192.168.1.1 and you will be asked for username and password. Fill this in and click *change password*
13. Set up the router according to your wishes and reboot
14. Do not forget to set your client back to automatic DHCP
15. Post your findings in the appropriate build thread (e.g.: https://forum.dd-wrt.com/phpBB2/viewtopic.php?t=320457)

Second/Subsequent Flashes

Once dd-wrt is installed, you can flash the appropriate *.bin* files.
It is not necessary to install a *.bin* file from the same build number as the *.img* file.

For Brainslayer builds use the *.bin* files from ftp://ftp.dd-wrt.com/betas/, choose year, build number and navigate to /netgear-r7800/

Resetting with: *nvram erase && reboot* from CLI is not strictly necessary when upgrading, just do it if you experience problems or if the build thread advises it to do.
Every new build has a build thread to report success and/or problems, which can be found in the Atheros forum: https://forum.dd-wrt.com/phpBB2/viewforum.php?f=28
This forum can also be used when asking for help with your R7800

Switching between builds from Kong and BS
You can usually switch between Kong's and BS's builds without a problem, just upload the normal .bin file via the GUI.
If you experience problems after uploading reset with *nvram erase && reboot* from CLI.

Going back from DDWRT to Stock Firmware

1. Use Internet Explorer, clear browser cache
2. Reset router to defaults using the GUI (*Administration/Factory defaults*)
3. There is a special file for going back to stock named: ddwrt-to-netgear-fw-R7800.bin
   It can be found here in this thread.
   This will get you back to Netgear FW 1.0.0.40.
4. Upload the modified Netgear stock firmware do **not** reset to defaults (do that later).
   When you login use the same username and password as you have set for DDWRT.
5. Reset to defaults (*ADVANCED/Administration/Backup Settings/Revert to factory default settings*), click *Erase*, the router will reboot, the username will now be *admin* again and password: *password*. Which can be used to login from 192.168.1.1.
6. If the radios are not available when flashing back to Netgear FW and having reset, head over to the wireless settings page and set the Security options to WPA2-PSK and enter a password, the radios started working and the password reverted to the Netgear default password, if this does not help then follow Kong's instructions:
   "Solution: Netgear partition needs to be cleaned using command:
   mtd erase netgear
   This command must be executed on a console after you flashed back to netgear fw.
   You should be able to enabled telnet via: http://192.168.1.1/debug.htm
   Alternatively you can run this command in a serial console, in case you have a USB-TTL adapter connected".

Recovery

Recovery including serial debricking is discussed in https://openwrt.org/toh/netgear/r7800
If you want to TFTP DDWRT use the .img files used for the first flash:

Recovery by TFTP

See: https://kb.netgear.com/000059633/How-to-upload-firmware-to-a-NETGEAR-router-using-TFTP-client and https://wiki.dd-wrt.com/wiki/index.php/TFTP_flash

To TFTP when not bricked, power-up holding the reset button to TFTP:

1. Set a static IP (e.g. IP address 192.168.1.9, subnet mask 255.255,255.0, default gateway 192.168.1.1)
2. In a TFTP client, use 192.168.1.1 as server, password blank, select DDWRT file for first flash or OEM Netgear firmware
3. Don't start TFTP yet...open a cmd window, run `ping -t 192.168.1.1` (for Windows; no '-t' for linux)
4. Press and hold the reset button and power up the router. Start the TFTP when ping replies with TTL
    - The thread says to look for TTL=100, but this has also worked when TTL=64 is seen
5. It should push the firmware, then wait and watch the lights and the pings, ne patient it can take a while
6. After a reboots, access the router on 192.168.1.1, be sure to detach the router from the network otherwise the router will search for another IP address, if you can not login then set your client to Automatically obtain IP address (DHCP) instead of the static IP in step 1.

Usefull information

If you want to read everything from the beginning start at page one of the *Netgear R7800 (Nighthawk X4S – AC2600) - status* and you can go up to page 177 at the moment: https://forum.dd-wrt.com/phpBB2/viewtopic.php?t=289788

Wireless settings

https://forum.dd-wrt.com/phpBB2/viewtopic.php?p=1154617#1154617
https://wiki.dd-wrt.com/wiki/index.php/QCA_wireless_settings
https://svn.dd-wrt.com/ticket/5699
https://w.wol.ph/2015/08/28/maximum-wifi-transmission-power-country/

Performance

Need link to set the core affinity, @tatsuya46 ?
https://forum.dd-wrt.com/phpBB2/viewtopic.php?p=1106357&sid=33cb7842f919aab497be48eeebd25927